1. Perform a full TCP port scan on your target and create an HTML report. Submit the number of the highest port as the answer.

```bash

┌─[eu-academy-5]─[10.10.14.223]─[htb-ac-1522420@htb-muk1cve8f5]─[~]

└──╼ [★]$ sudo nmap 10.129.211.152 -p- -oA khanh

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-17 10:47 CST

Stats: 0:01:51 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan

SYN Stealth Scan Timing: About 58.16% done; ETC: 10:50 (0:01:21 remaining)

Nmap scan report for 10.129.211.152

Host is up (0.24s latency).

Not shown: 65528 closed tcp ports (reset)

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

110/tcp open pop3

139/tcp open netbios-ssn

143/tcp open imap

445/tcp open microsoft-ds

31337/tcp open Elite

```

Cổng của máy chủ đích là 31337

P/s : 31337